

# Public-key Infrastructure

---

**Clemente Galdi**

Dipartimento di Scienze Fisiche  
Università di Napoli "Federico II"

[c.galdi@na.infn.it](mailto:c.galdi@na.infn.it)



# Distribuzione chiavi pubbliche

- Come vengono distribuite le chiavi pubbliche?
- Chi ci assicura che una chiave pubblica è quella di un prefissato utente?



# Distribuzione chiavi pubbliche

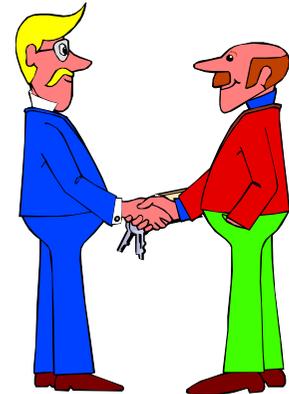
## Alcune tecniche:

- Invio point-to-point su canale fidato
- Annuncio pubblico
- Directory disponibile pubblicamente
- Autorità per le chiavi pubbliche
- Certificati per le chiavi pubbliche



# Invio point-to-point su canale fidato

- Esempi: scambio diretto, uso di un corriere fidato,...
- Oppure
  - invio su canale pubblico
  - autenticazione (per esempio: hash su canale fidato)



## Va bene se:

- Uso non frequente
- Piccoli sistemi

# Annuncio pubblico

- Invio ad altri utenti / Broadcast chiave
- Esempio: aggiunta della chiave pubblica PGP ai messaggi inviati a forum pubblici

**Problema: ci dobbiamo fidare dell'annuncio?**



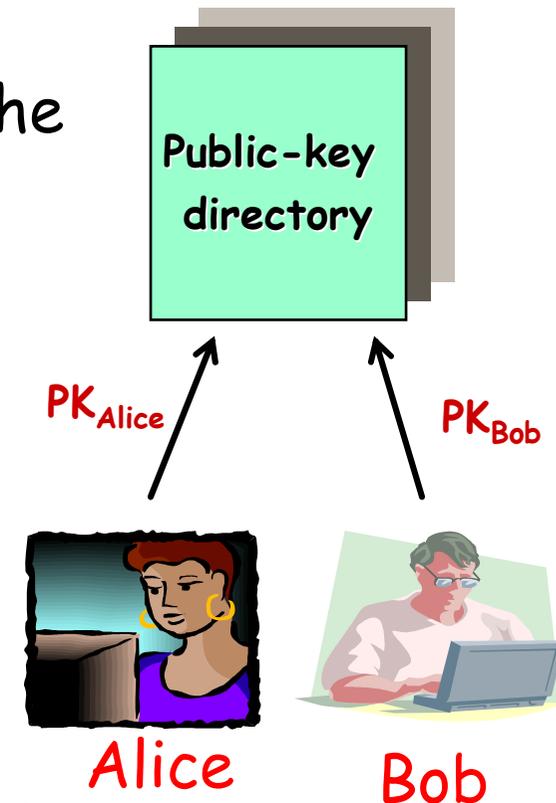
# Directory disponibile pubblicamente

## Entità fidata:

- Gestisce la directory di chiavi pubbliche

## Ogni partecipante:

- Registra la propria chiave pubblica
  - Di persona o in modo autenticato
- Può aggiornare la propria chiave
  - Se usata da troppo tempo o chiave privata compromessa
- Può accedere alla directory
  - Necessaria comunicazione sicura ed autenticata



# Autorità per le chiavi pubbliche

- Gestisce directory chiavi pubbliche
- Ha una chiave pubblica nota a tutti gli utenti
- Ogni utente chiede la chiave pubblica desiderata, l'autorità la invia
- Svantaggi:
  - server on-line
  - collo di bottiglia

Vediamo un possibile protocollo

# Autorità per le chiavi pubbliche

Public-key  
Authority

Voglio la chiave  
pubblica di Bob

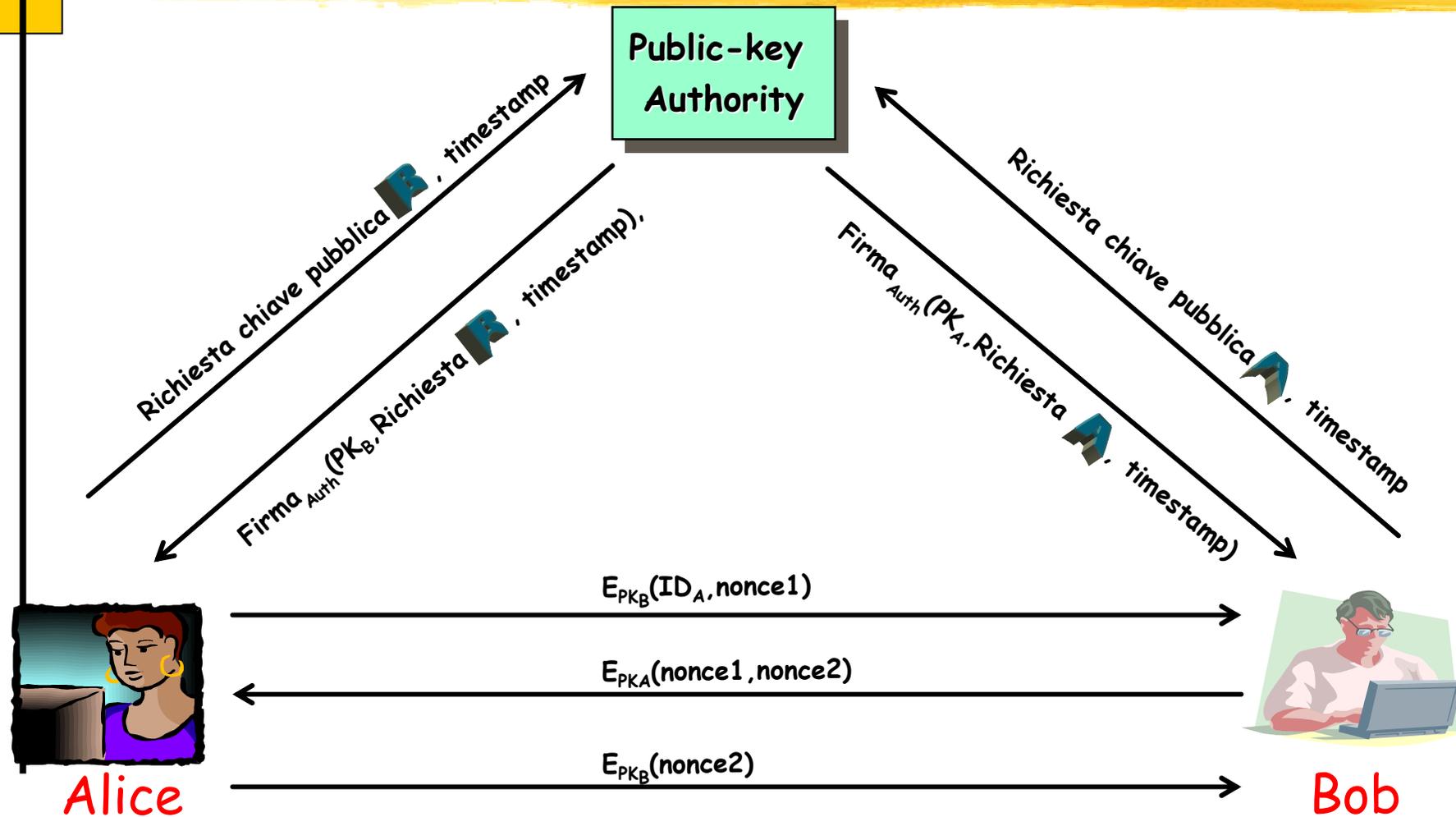


Alice



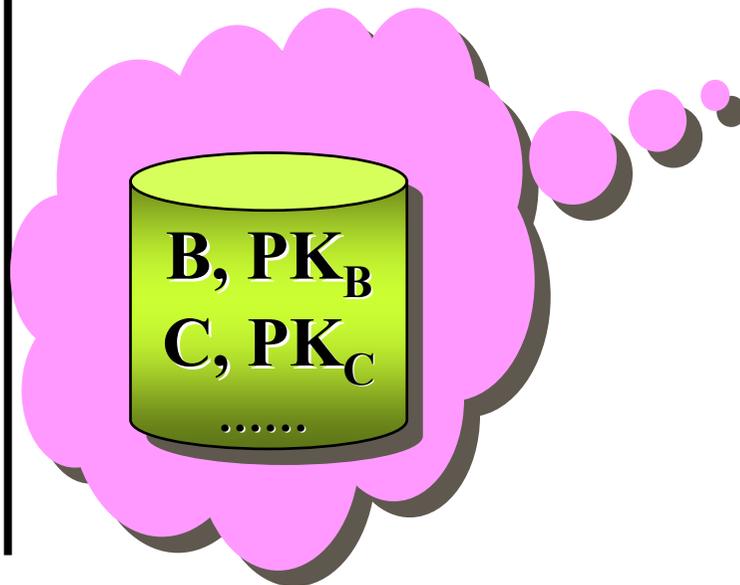
Bob

# Autorità per le chiavi pubbliche



# Caching chiavi pubbliche

Ottenuta una chiave pubblica, si memorizza



Alice

... ma occorre aggiornarla periodicamente

# Certificati

## Mondo fisico

- Carta di identità
  - Un' **autorità riconosciuta** lega un nome ad una foto



## Mondo digitale

- Certificato digitale
  - Un' **autorità riconosciuta** lega un nome ad una chiave pubblica



# Certificati



**Autorità di Certificazione:**  
Terza parte fidata la cui firma  
garantisce il legame tra chiave  
ed identità

Alcune proprietà dei certificati:

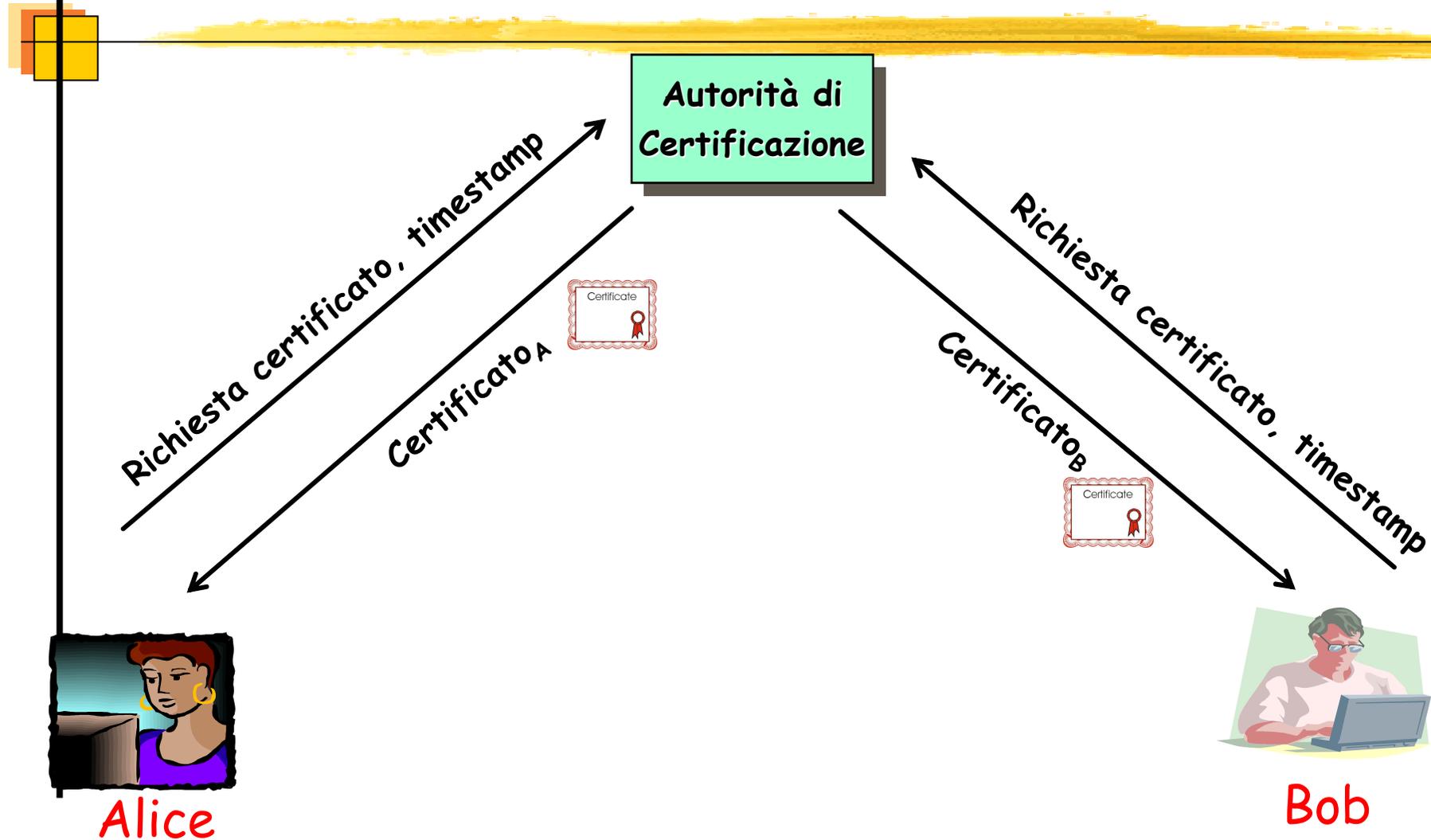
- Ognuno può leggerli e determinare nome e chiave pubblica
- Ognuno può verificarli ed assicurarsi dell'autenticità
- Solo l'Autorità può crearli ed aggiornarli

# Certificati

- Esempi di altri dati in un certificato:
  - periodo di validità chiave pubblica
  - numero seriale o identificatore chiave
  - info aggiuntive su chiave (ad es., algoritmi ed utilizzo)
  - info aggiuntive su utente
  - stato della chiave pubblica
- Formato più diffuso: definito dallo standard internazionale **ITU-T X.509**

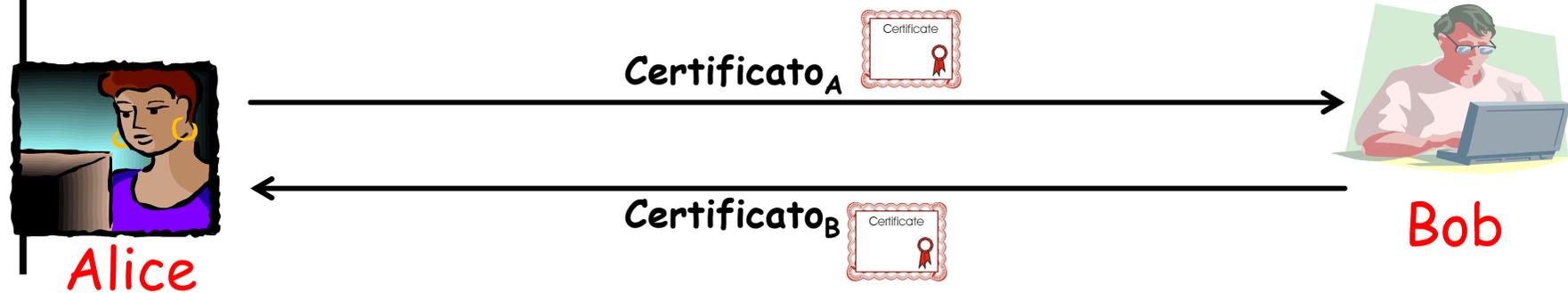


# Richiesta Certificati



# Scambio Certificati

Autorità  
Certificazione



# Revoca di certificati

- Che succede se la chiave privata viene compromessa?
- L'utente può richiedere la **revoca** del certificato



# Revoca Certificati: Motivi

- Compromissione chiave privata
- Info non più valide (es., cambio affiliazione)
- Non più utile per lo scopo prefissato
- Compromissione algoritmo
- Perdita o malfunzionamento di security token, perdita di password o PIN
- Cambio politiche di sicurezza
  - (es., la CA non supporta più servizi per certificati)

# Revoca Certificati: Metodi

- Data scadenza dentro un certificato
  - Certificati "a breve scadenza"
- Notifica manuale
  - Informazione tramite canali speciali
  - Solo per sistemi piccoli o chiusi
- File pubblico di chiavi revocate
  - Certificate Revocation List (CRL)
- Certificato di revoca
  - Sostituisce certificato revocato nella directory

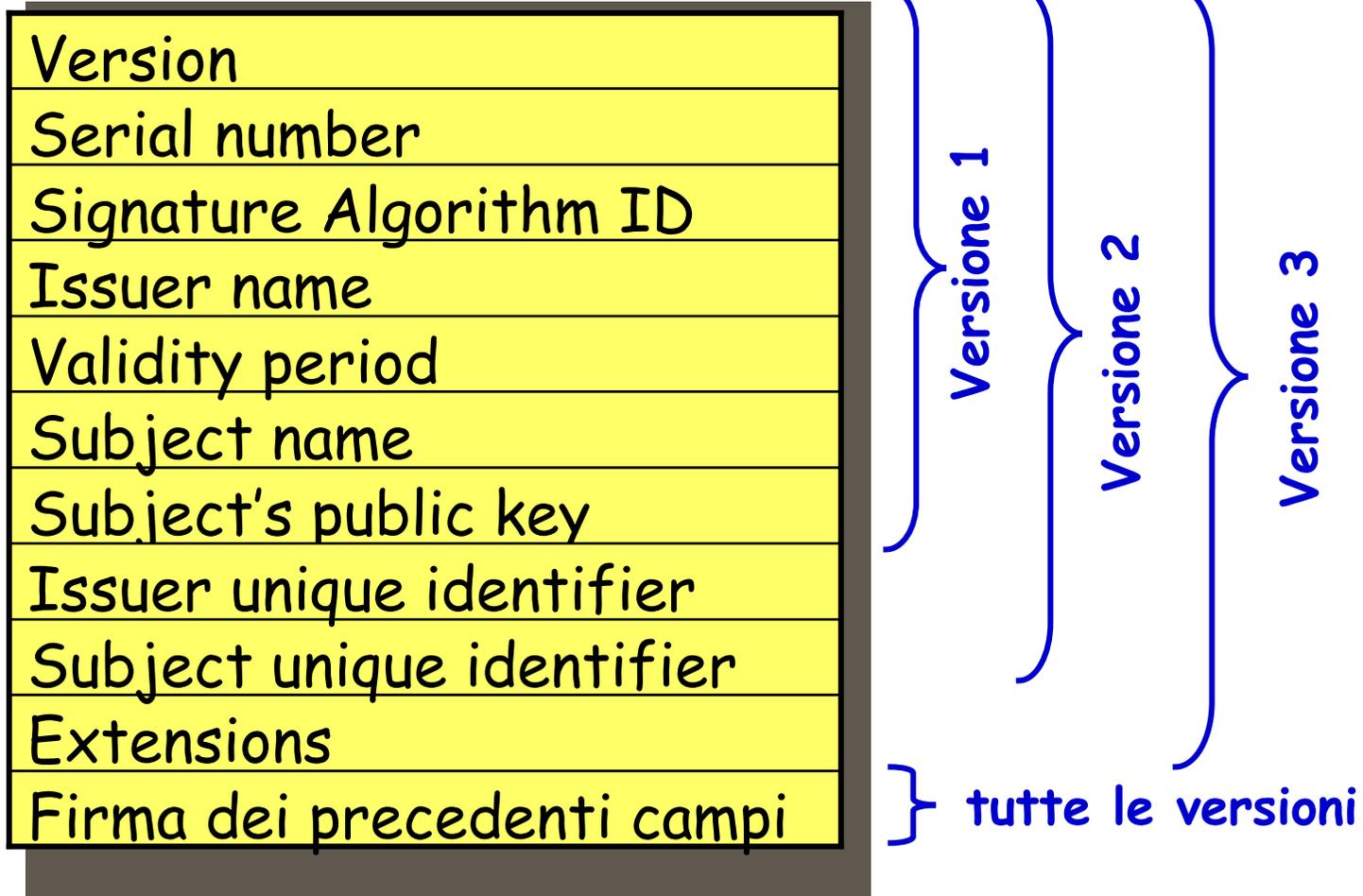
# Certificate Revocation List (CRL)

- Lista firmata dalla CA contenente:
  - numeri seriali dei certificati emessi revocati
    - (ma non ancora scaduti)
  - quando è avvenuta la revoca
  - altro (per es., motivi)
- La data della CRL indica quanto sia aggiornata

# Standard dei certificati X.509

- Più diffuso ed utilizzato standard per i certificati
- Parte della serie X.500 di raccomandazioni che definisce un "directory service"
  - directory: server o insieme distribuito di server che mantiene un database di informazioni su utenti
- Definito nel 1988 da ITU-T, modificato nel 1993 e 1995
  - International Telecommunication Union, Telecommunication Standardization Sector
- Usato in molte applicazioni
  - S/MIME, SSL/TLS, SET, IPSEC, ...

# Certificati X.509



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |

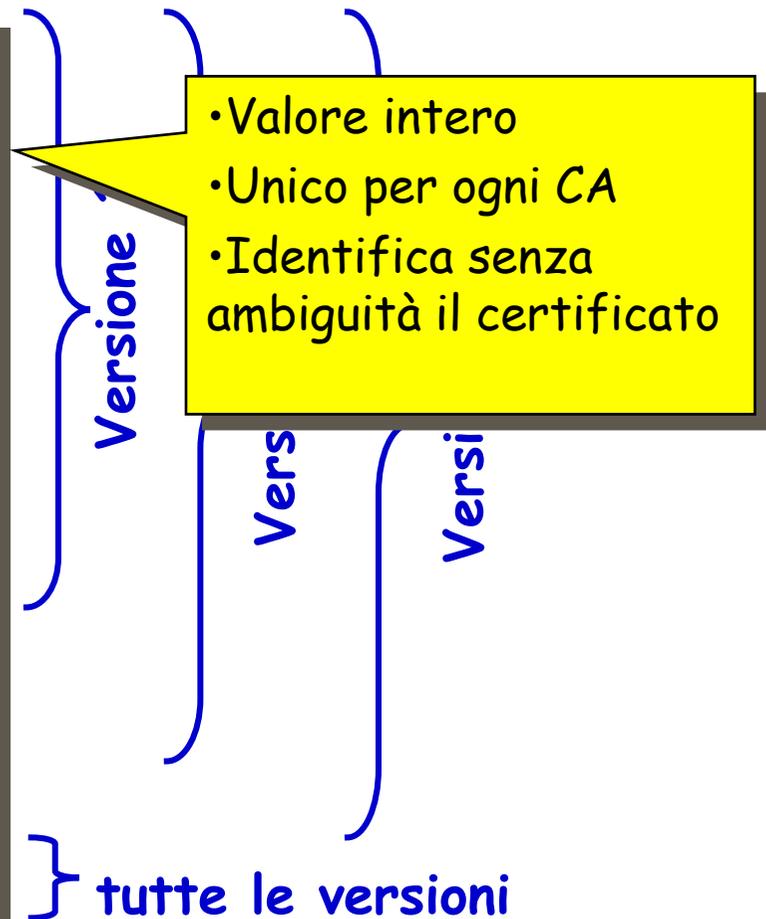
Versione 1

- 1 default
- 2 se presente "Issuer unique identifier" oppure "Subject unique identifier"
- 3 se ci sono estensioni

tutte le versioni

# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |

•Nome X.500 della CA che ha creato e firmato il Certificato

Versione 1

Versione 2

Versione 3

tutte le versioni

# Nome X.500

Sequenza di coppie nome-valore che identificano univocamente un'entità

`uid=doe,e=doe@netscape.com,cn=John Doe,o=Netscape Communications Corp.,c=US`

**email**

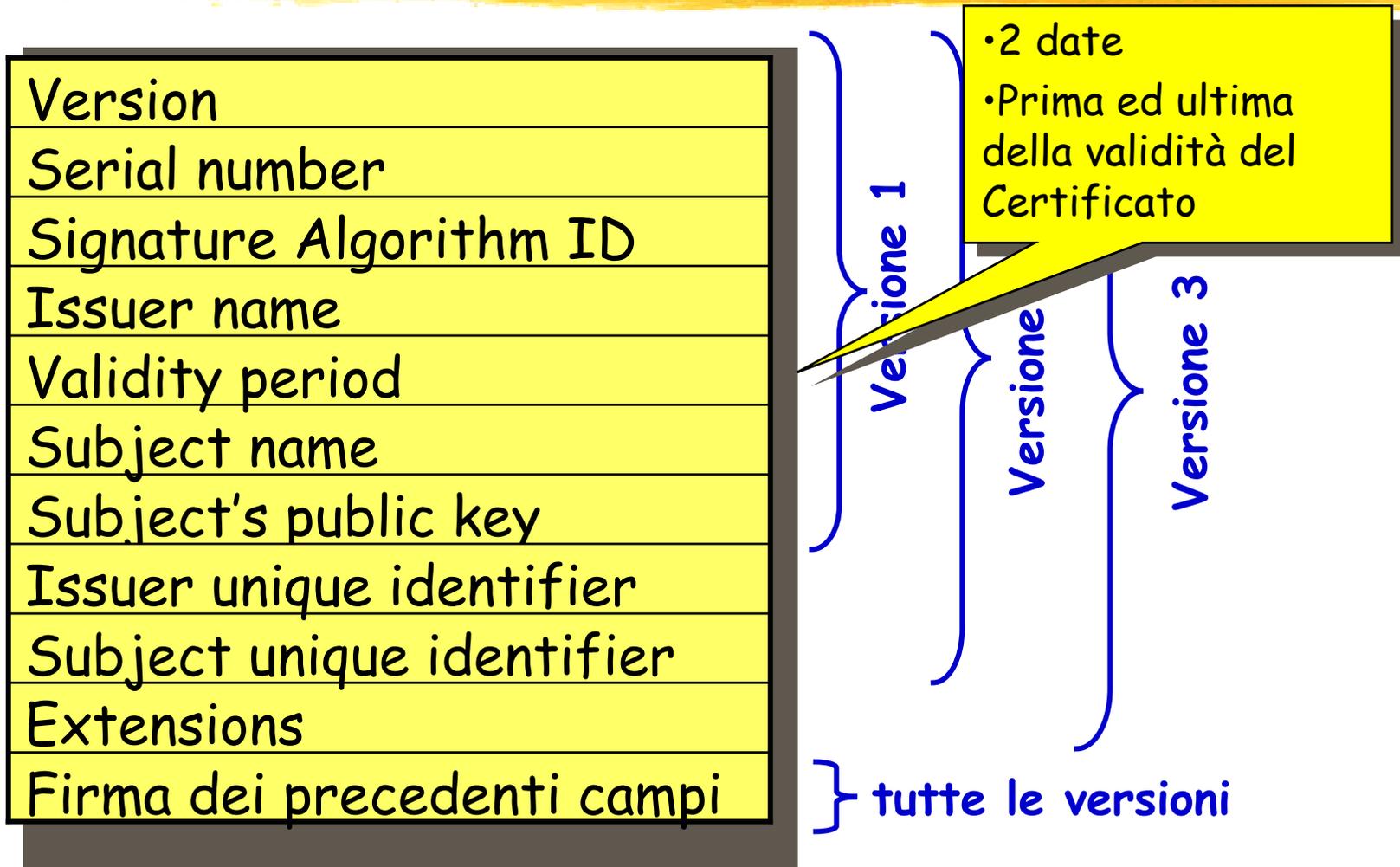
**ID utente**

**Nome comune utente**

**organizzazione**

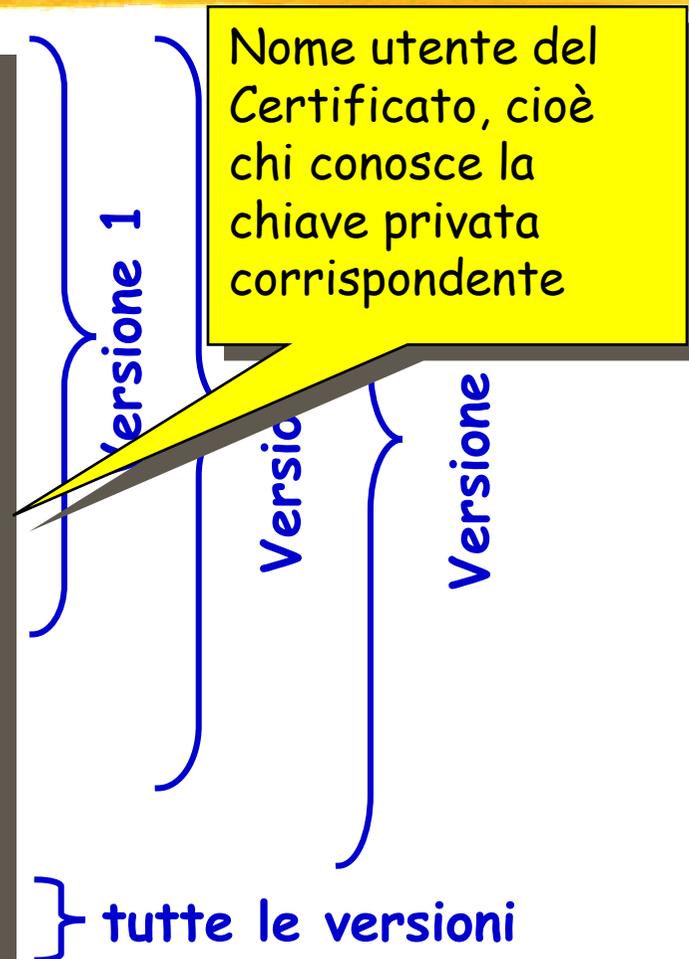
**nazione**

# Campi Certificati X.509



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |

- Chiave pubblica del soggetto
- Identificativo algoritmo e parametri associati

Versione 1

Versione

Versione

} tutte le versioni

# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |

Versione 1

- Opzionale
- Stringa di bit utile per identificare la CA che ha emesso il Certificato nel caso che il nome X.500 sia stato riutilizzato

Vers

} tutte le versioni

# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |

Versione 1

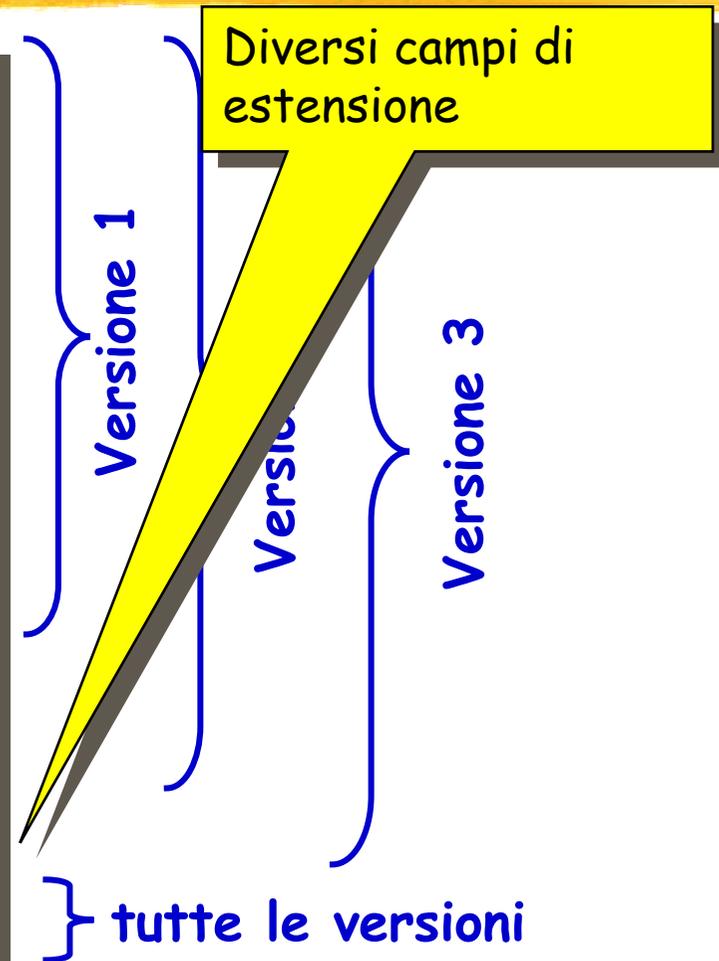
- Opzionale
- Stringa di bit utile per identificare il soggetto nel caso che il nome X.500 sia stato riutilizzato

Versione

} tutte le versioni

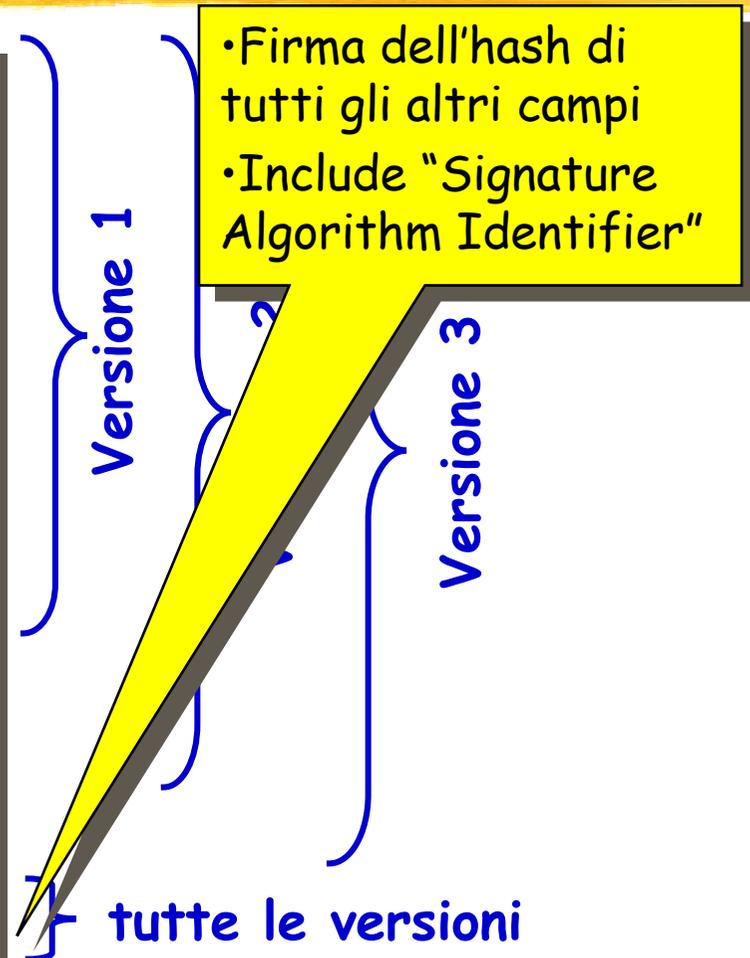
# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |



# Campi Certificati X.509

|                            |
|----------------------------|
| Version                    |
| Serial number              |
| Signature Algorithm ID     |
| Issuer name                |
| Validity period            |
| Subject name               |
| Subject's public key       |
| Issuer unique identifier   |
| Subject unique identifier  |
| Extensions                 |
| Firma dei precedenti campi |



# Esempio

## Certificate:

### Data:

Version: v3 (0x2)

Serial Number: 3 (0x3)

Signature Algorithm: PKCS #1 MD5 With RSA Encryption

Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US

### Validity:

Not Before: Fri Oct 17 18:36:25 1997

Not After: Sun Oct 17 18:36:25 1999

Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US

### Subject Public Key Info:

Algorithm: PKCS #1 RSA Encryption

### Public Key:

#### Modulus:

00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:  
ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:  
43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:  
98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:  
73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:  
9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:  
7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:  
91:f4:15

Public Exponent: 65537 (0x10001)

### Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36: 26:c9

### Signature:

Algorithm: PKCS #1 MD5 With RSA Encryption

### Signature:

6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:  
30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:  
f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:  
2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:  
b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:  
4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:dd:c4

# Certificato in 64-byte-encoded form

-----BEGIN CERTIFICATE-----

```
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
MA8GA1UEChMITmV0c2NhcGUxFTATBgNVBAsTDfN1cHJpeWEncyBDQTAeFw05NzEw
MTgwMTM2MjVhFw05OTEwMTgwMTM2MjVhMEgxCzAJBgNVBAYTAIVTMREwDwYDVQQK
EwhOZXZRzY2FwZTENMAAsGA1UECxEUHViczEXMBUGA1UEAxMOU3Vwcm15YSBTaGV0
dHkkgZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRjgEjmKiqG
7SdATYazBcABu1AVyd7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
QZBcrXpc0k4du+2Q6xJu2MPm/8WKuMOnTuvzpo+SGXelmHVChEqooCwfdiZywyZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAfBgNV
HSMEGDAWgBTy8gZZkBhHUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBgQBt
6/z07Z635DfzX4XbAFpjlRI/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3
UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A==
```

-----END CERTIFICATE-----

# Notazione dello standard

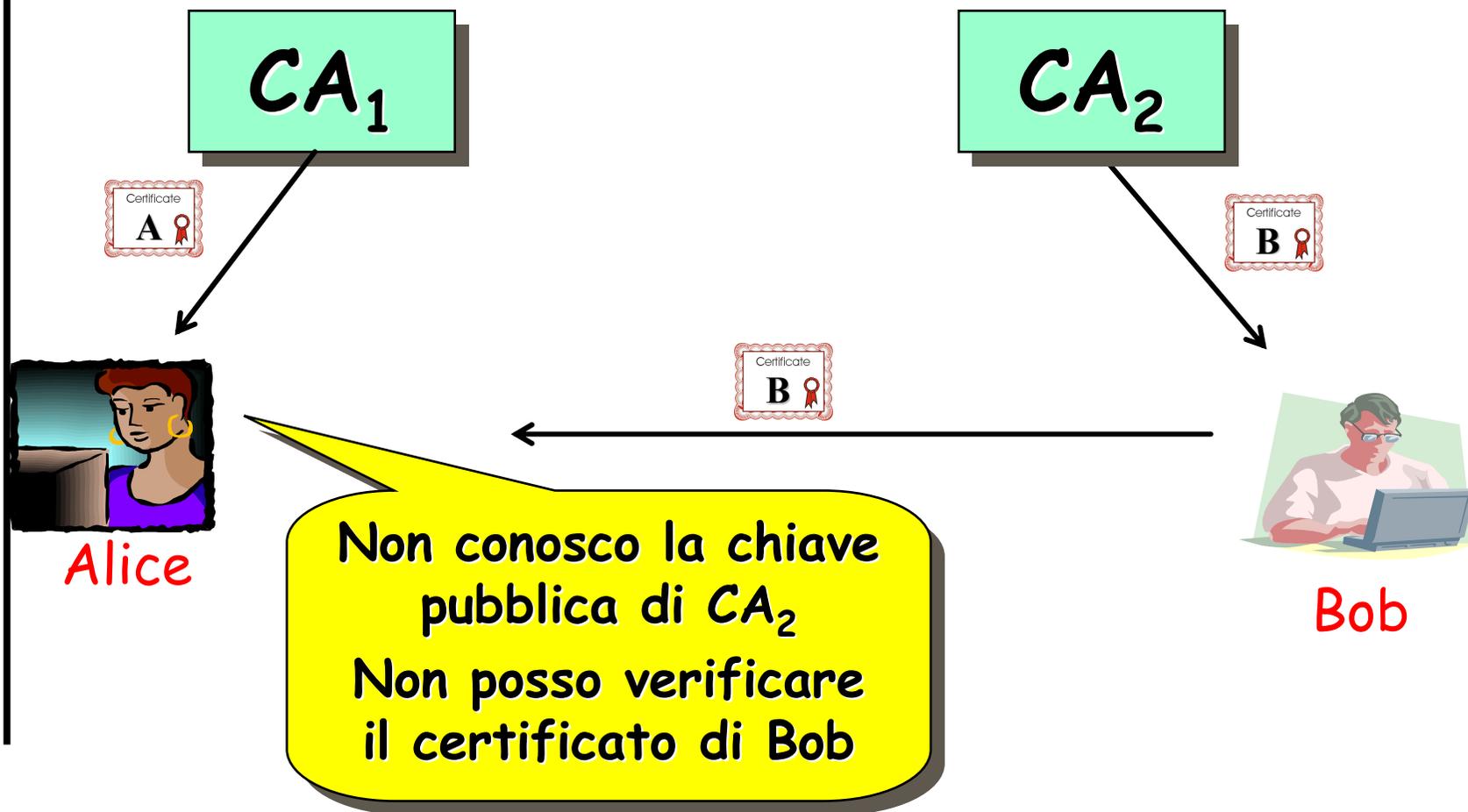
➤  $Y \ll X \gg$

➤ certificato utente  $X$  creato dalla Autorità  $Y$

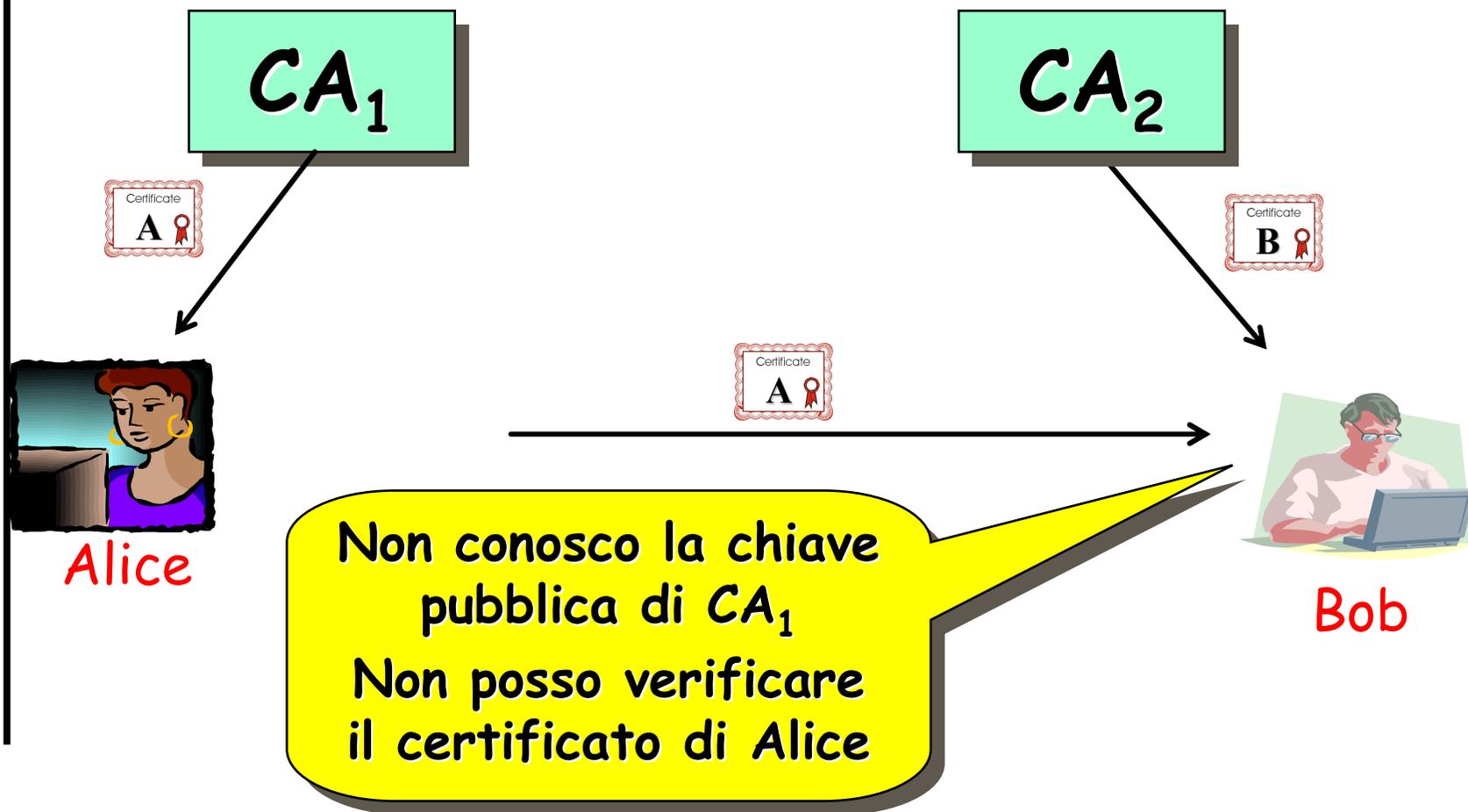
➤  $Y \{ I \}$

➤ Firma dell'hash di  $I$  da parte di  $Y$

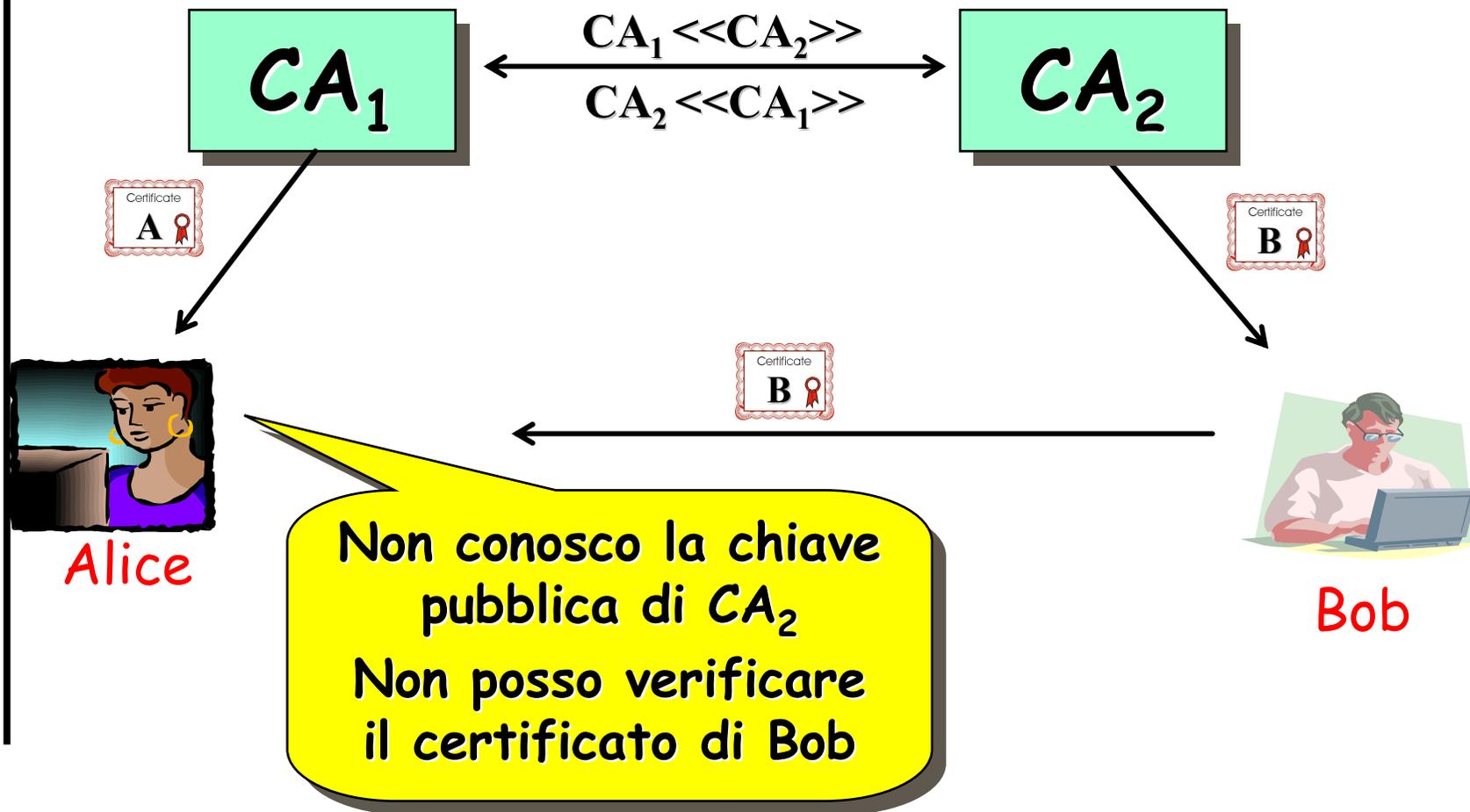
# Diverse CA



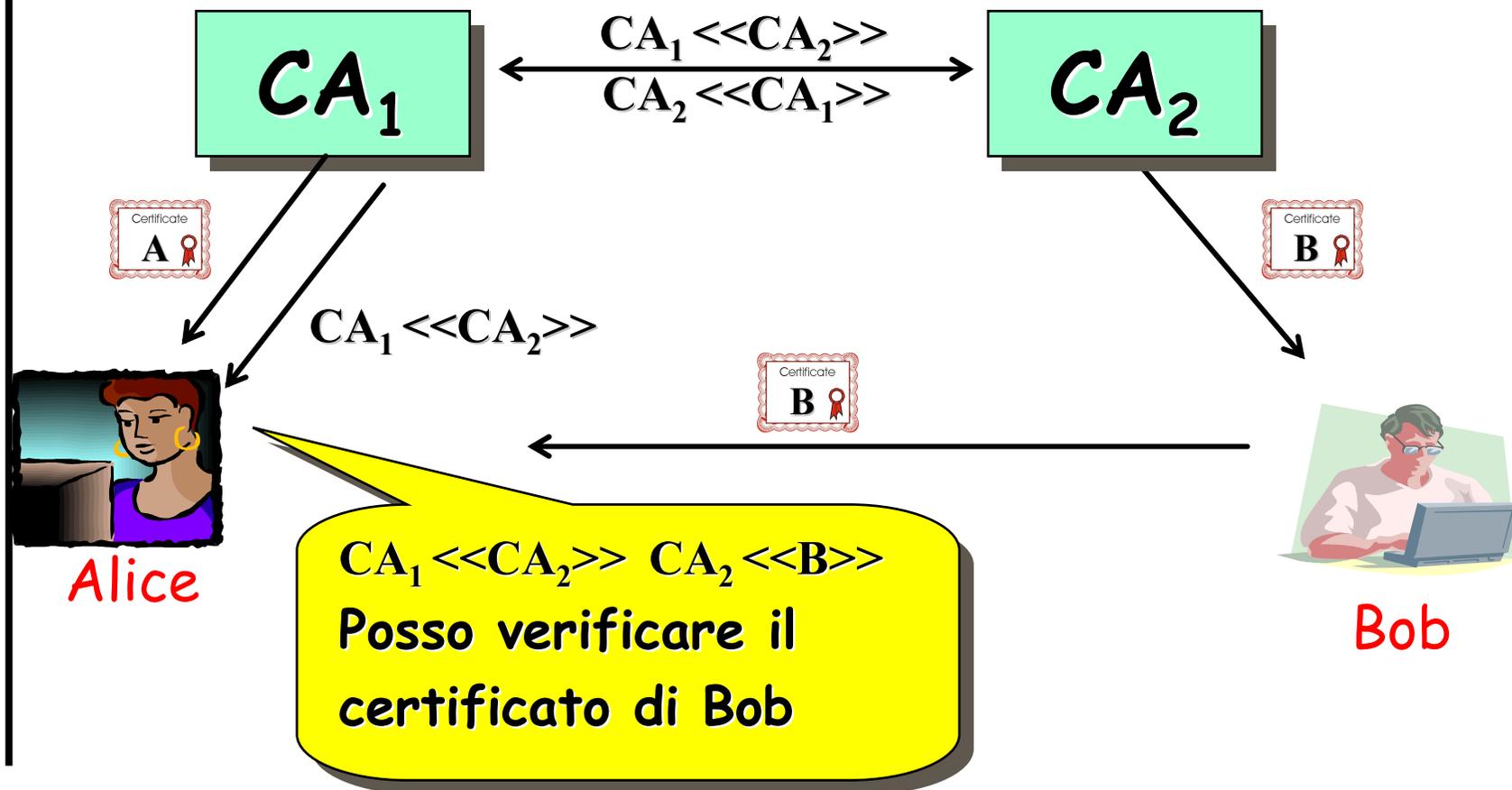
# Diverse CA



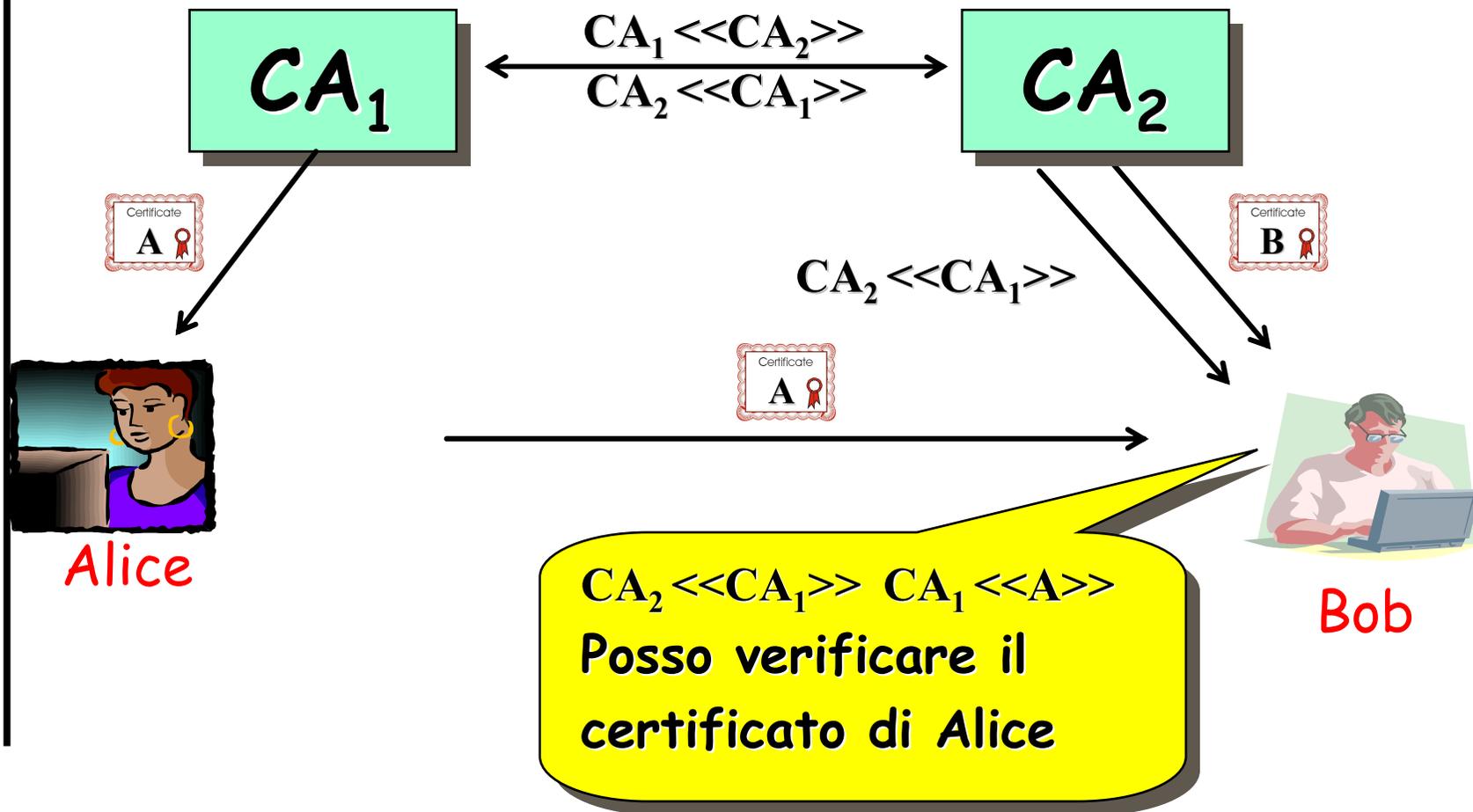
# Diverse CA



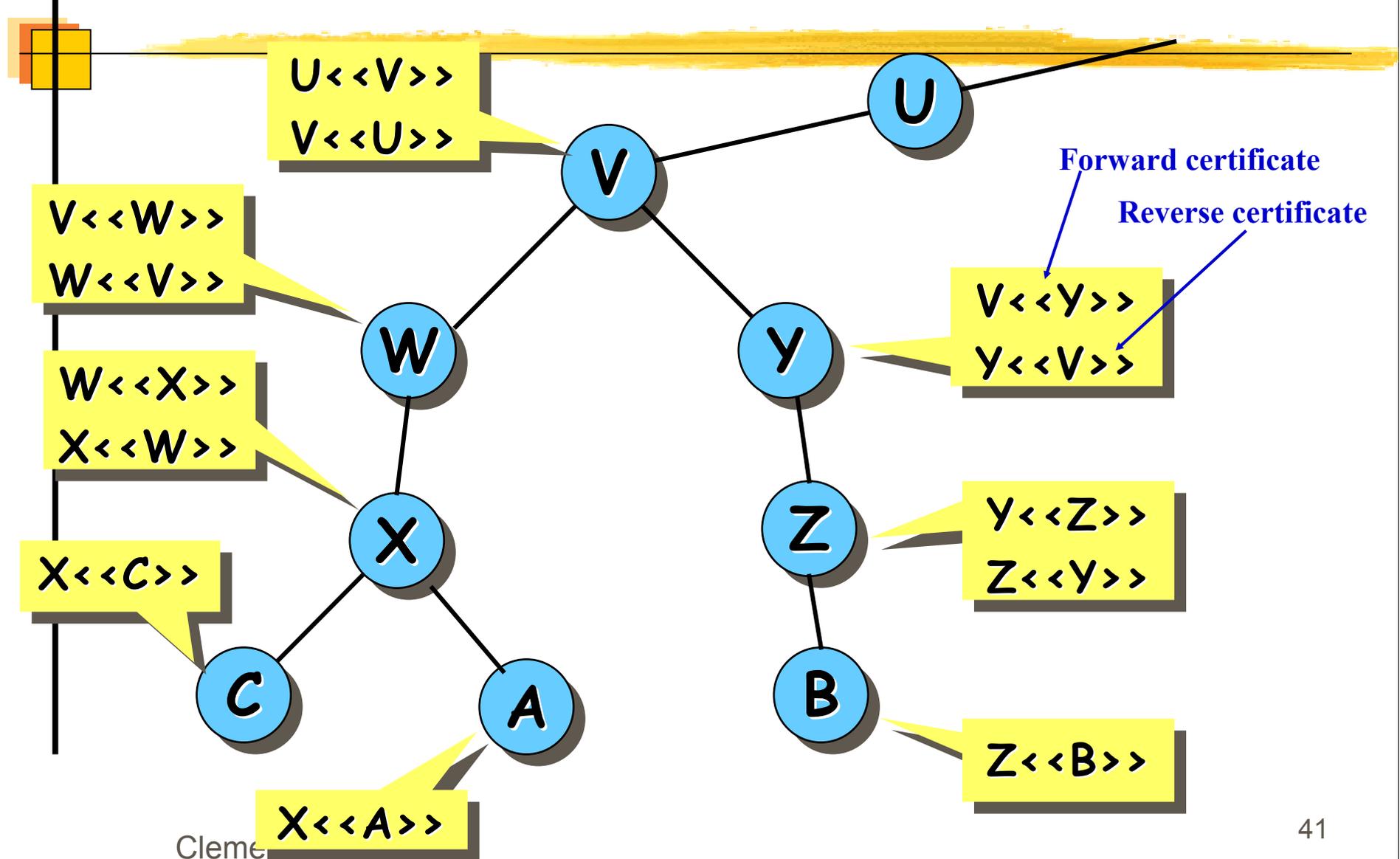
# Diverse CA



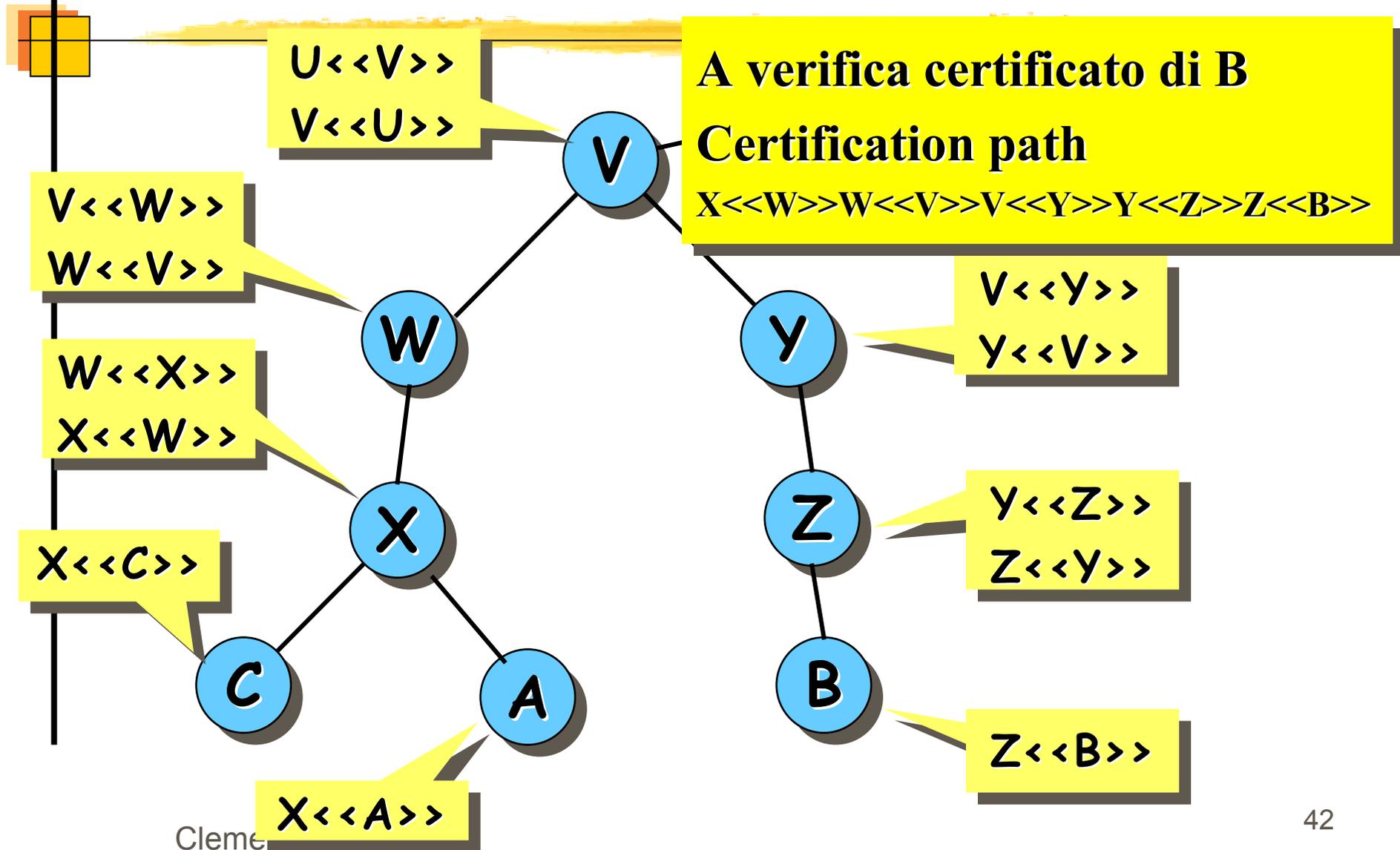
# Diverse CA



# Gerarchia X.509



# Gerarchia X.509



# Revoca di certificati

- Ogni CA mantiene lista dei propri certificati che sono stati revocati ma non scaduti
- Bisogna controllare se un certificato non sia stato revocato
- Caching dei certificati revocati

# CRL

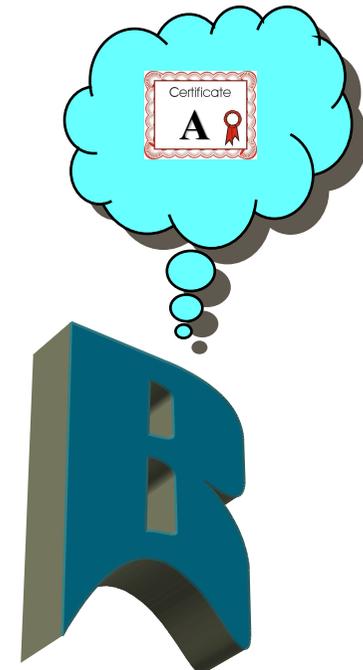
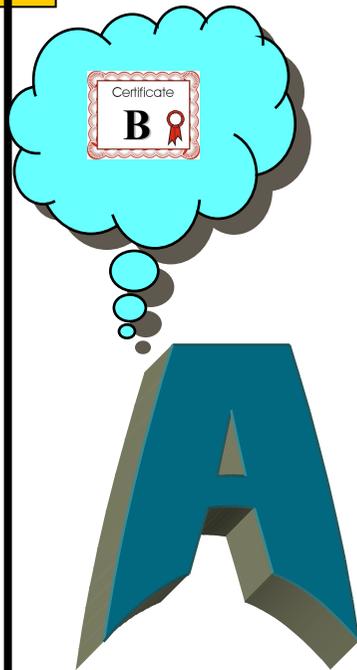
|                                 |                               |
|---------------------------------|-------------------------------|
| Signature Algorithm Identifier  |                               |
| Issuer name                     |                               |
| Data di questo aggiornamento    |                               |
| Data del prossimo aggiornamento |                               |
| User certificate serial number  | } <b>Certificato revocato</b> |
| Data della revoca               |                               |
| ...                             |                               |
| User certificate serial number  | } <b>Certificato revocato</b> |
| Data della revoca               |                               |
| Firma                           |                               |

# Autenticazione X.509

X.509 fornisce anche tre procedure di autenticazione:

- Autenticazione One-way
- Autenticazione Two-way
- Autenticazione Three-way

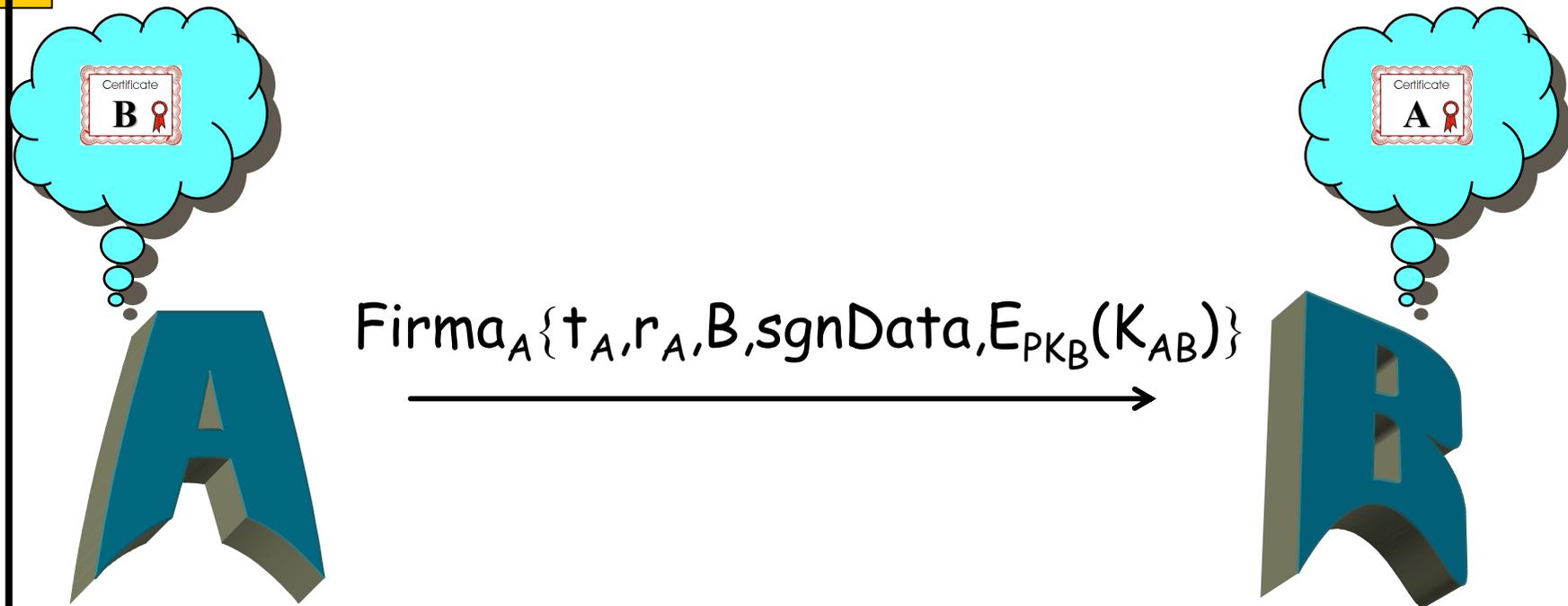
# Autenticazione X.509



**Assumiamo che entrambi conoscano le chiavi pubbliche**

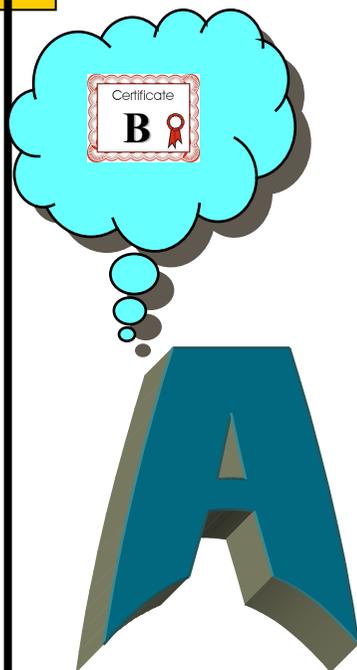
- Scambio dei certificati come primo messaggio, oppure
- Certificati ottenuti dalla directory

# Autenticazione One-way



- Messaggio di A
- Diretto a B
- Integrità ed originalità (non inviato più volte) messaggio

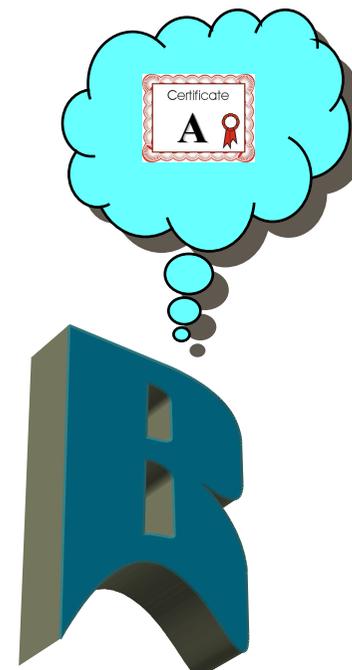
# Autenticazione One-way



Timestamp:  
• Expiration time

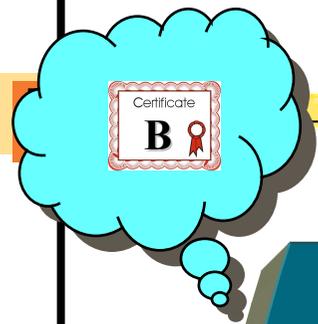
nonce

$\text{Firma}_A \{ t_A, r_A, B, \text{sgnData}, E_{PK_B}(K_{AB}) \}$



Opzionali  
sgnData: info per B  
 $K_{AB}$ : session key

# Autenticazione One-way



A

$\text{Firma}_A\{t_A, r_A, B, \text{sgnData}, E_{PK_B}(K_{AB})\}$



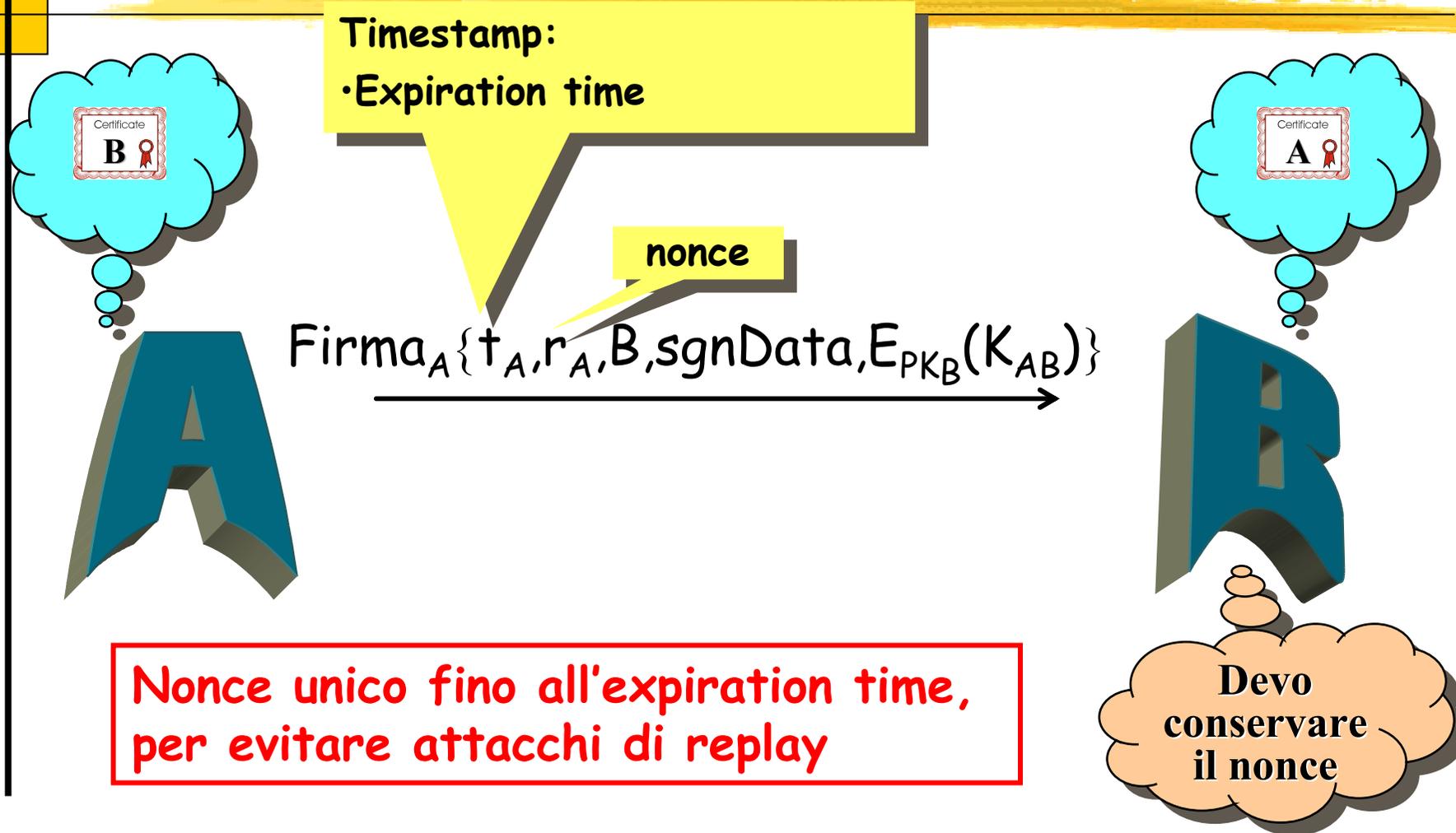
B



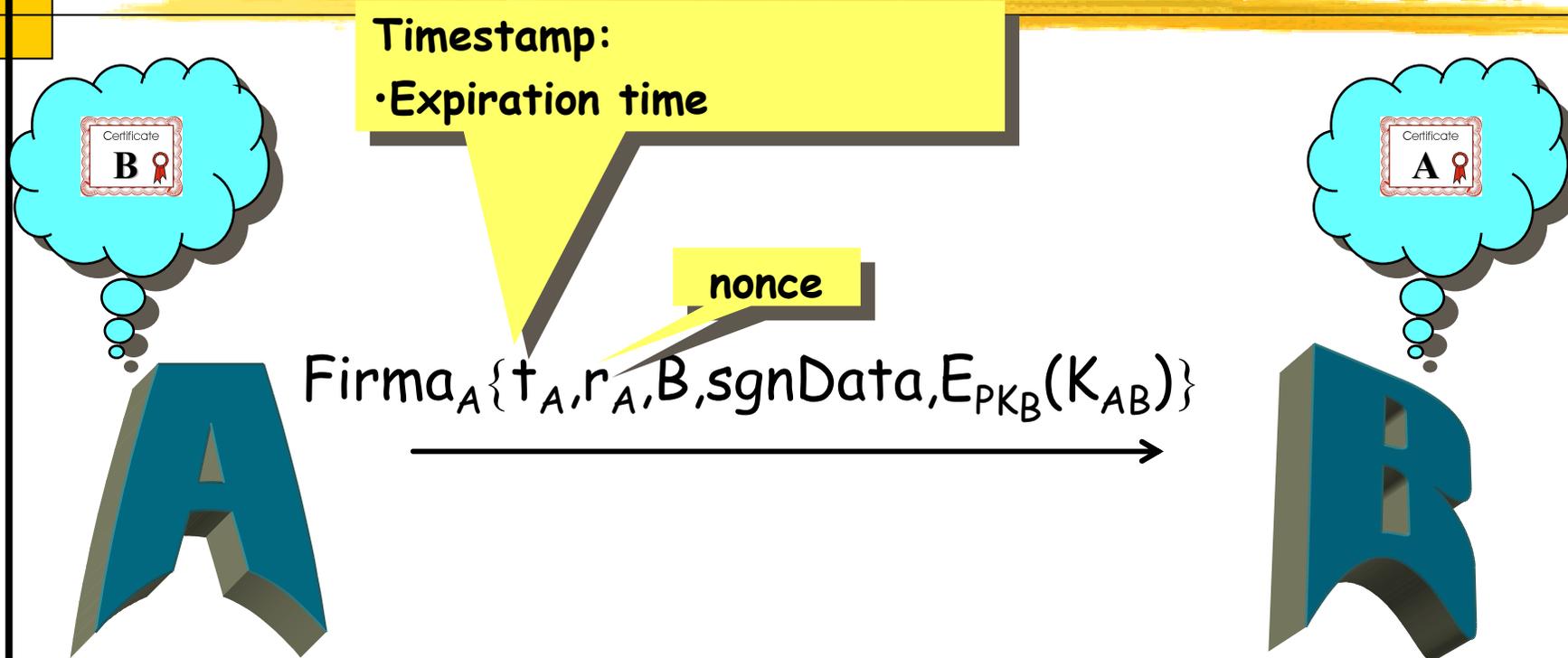
$\text{Firma}_A\{t_A, r_A, B, \text{sgnData}, E_{PK_B}(K_{AB})\}$



# Autenticazione One-way

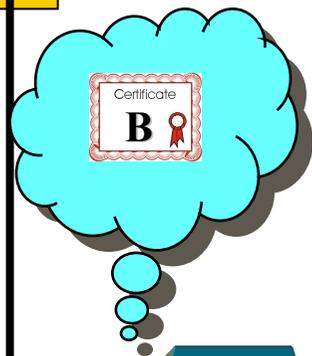


# Autenticazione One-way



- Messaggio di A
- Diretto a B
- Integrità ed originalità (non inviato più volte) messaggio

# Autenticazione Two-way



A

$Firma_A\{t_A, r_A, B, sgnData, E_{PK_B}(K_{AB})\}$



$Firma_B\{t_B, r_B, A, r_A, sgnData, E_{PK_A}(K_{BA})\}$



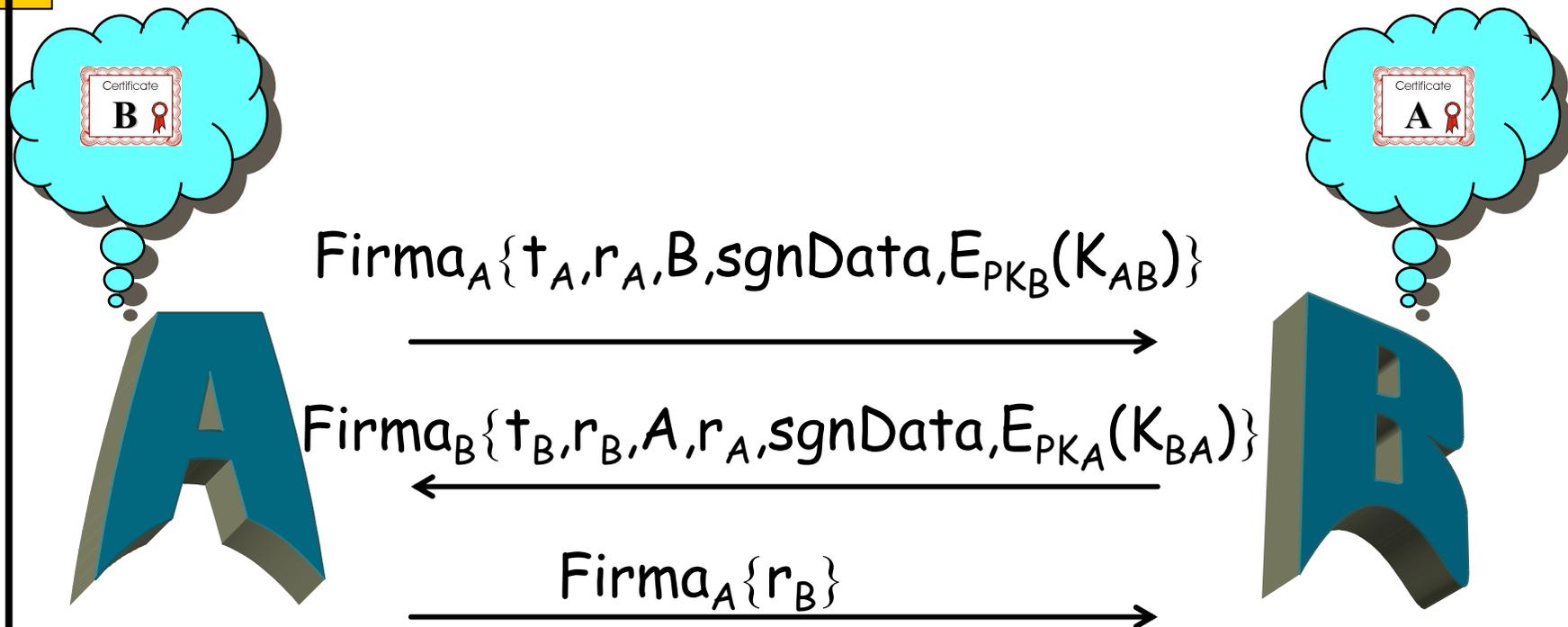
opzionali



B

Messaggio di B  
Diretto ad A  
Integrità ed originalità messaggio di B

# Autenticazione Three-way



Scopo: Eliminare il check dei timestamp  
Necessario in assenza di clock sincronizzato

# X.509 versione 3

## Requisiti non soddisfatti dalla versione 2 [W. Ford 1995]

- Subject field non adeguato: nomi X.509 sono corti, e mancano dettagli identificativi che potrebbero essere utili
- Subject field non adeguato per le applicazioni che riconoscono entità dall'indirizzo email, URL
- Vi è necessità di indicare politiche di sicurezza
- Vi è necessità di limitare il danno che potrebbe fare una CA maliziosa, ponendo vincoli all'applicabilità di un particolare certificato
- E' importante distinguere chiavi diverse usate dallo stesso utente in tempi diversi

# X.509 versione 3

## Estensioni opzionali nella versione 3

- Soluzione flessibile
- Meglio dell'aggiungere altri campi fissi alla versione 2

## Ogni estensione contiene:

- Identificatore estensione
- Indicatore di criticità
- Valore estensione

•Indica se l'estensione può essere ignorata

•Se TRUE e l'implementazione non riconosce l'estensione allora deve trattare il certificato come non-valido

# Categorie Estensioni

Tre categorie principali per le estensioni:

- Key and Policy Information
- Certificate Subject and Issuer Attributes
- Certification Path Constraints

# Key and Policy Information

## Authority key identifier

indica quale di più chiavi pubbliche della CA usare per verificare la firma di un certificato o della CRL

## Subject key identifier

identifica quale di più chiavi pubbliche viene certificata

## Key usage

restrizione sull'uso della chiave certificata, come scopo:  
(digital signature, key encryption, data encryption, key agreement, CA signature verification on certificates, CA signature verification on CRL)

# Key and Policy Information

## Private-key usage period

periodo uso della chiave privata (per la firma, diverso periodo per chiave privata e pubblica)

## Certificate policy

insieme di regole che indica l'applicabilità di un certificato ad una comunità e/o classi di applicazioni con requisiti di sicurezza comuni

## Policy mappings

usato solo per CA da altre CA. Permette ad una CA di indicare che una propria politica può essere considerata equivalente ad un'altra politica usata dalla CA soggetto.

# Certificate Subject and Issuer Attributes

## Subject alternative name

contiene uno o più nomi alternativi, in formati alternativi.  
Importante per le applicazioni che hanno formati propri  
per i nomi (ad es., email, IPSec)

## Issuer alternative name

contiene uno o più nomi alternativi, in formati alternativi

## Subject directory attributes

contiene attributi della directory X.500 per il soggetto  
del certificato

# Certification Path Constraints

## Basic constraints

indica se il soggetto può agire come CA. Se si, si possono specificare vincoli sulla lunghezza della certification path

## Name constraints

indica uno spazio dei nomi in cui tutti i seguenti certificati in un certification path devono essere

## Policy constraints

inibisce policy mappings per la parte rimanente della certification path

# Legislazione italiana



- Legge 15 marzo 1997 n. 59 "**Bassanini 1**" art. 15 comma 2:
  - *gli atti, i dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici e telematici, sono **validi e rilevanti ad ogni effetto di legge***
- Regolamento attuativo DPR 513/97, G.U. n° 60 13/3/1998
- Regolamento tecnico “*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici...*” Decreto del Presidente del Consiglio dei Ministri, G.U. n° 87 del 15/4/1999

# DPR 513/97, Art. 1



**a) firma digitale:** risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

...

**h) certificazione:** risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;

...

**k) certificatore:** soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;

# DPR 513/97, Art. 5



- 1. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di **scrittura privata** ai sensi dell'articolo 2702 del codice civile.*
- 2. Il documento informatico munito dei requisiti previsti dal presente regolamento ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile e soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.*

# DPR 513/97, Art. 8



3. ... le attività di certificazione sono effettuate da **certificatori** inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati nel decreto di cui all'articolo 3:

- a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati;
- b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;
- c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 3;
- d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.

# Regolamento Tecnico

## I. Regole di base

*RSA, DSS, chiave  $\geq 1024$  bit, SHA-1, RIPEMD-160*

## II. Regole per la certificazione delle chiavi

## III. Regole per la validazione temporale e per la protezione dei documenti informatici

## IV. Regole tecniche per le Pubbliche Amministrazioni

## V. Disposizioni finali

Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio  
del 13 dicembre 1999  
relativa ad un quadro comunitario per le firme elettroniche

## Art. 2 - Definizioni

- 1) *"firma elettronica", dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione;*
- 2) *"firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:*
  - a) *essere connessa in maniera unica al firmatario;*
  - b) *essere idonea ad identificare il firmatario;*
  - c) *essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;*
  - d) *essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.*

Attuazione della direttiva 1999/93/CE relativa ad un quadro  
comunitario per le firme elettroniche  
G.U. n. 39 del 15 febbraio 2002

**Art. 2**

- a) *"firma elettronica" l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;*
- d) *"certificati elettronici" gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;*
- e) *"certificati qualificati" i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva;*
- g) *"firma elettronica avanzata" la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;*

Attuazione della direttiva 1999/93/CE relativa ad un quadro  
comunitario per le firme elettroniche  
G.U. n. 39 del 15 febbraio 2002

## Art. 6

...

3. *Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre **piena prova**, fino a querela di falso, **della provenienza** delle dichiarazioni da chi l'ha sottoscritto.*

# Bibliografia

- **Cryptography and Network Security**  
by W. Stallings (2003)
  - cap. 10 (Key Management)
  - cap. 14 (X.509 Authentication Service)